CVE-2023-20849

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-20849
State	PUBLIC
Assigner	security@mediatek.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-04 03:15:00 UTC
Updated	2023-09-07 14:44:00 UTC
Description	In imgsys_cmdq, there is a possible use after free due to a missing valid range checking. This could lead to local escalation

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	11.0	All	All	All
Operating System	Google	Android	12.0	All	All	All
Operating System	Linux	Linux Kernel	6.1	-	All	All
Application	Linuxfoundation	Yocto	4.0	All	All	All
Application	Mediatek	Iot Yocto	23.0	All	All	All
Hardware	Mediatek	Mt2713	-	All	All	All
Hardware	Mediatek	Mt6895	-	All	All	All
Hardware	Mediatek	Mt6897	-	All	All	All
Hardware	Mediatek	Mt6983	-	All	All	All
Hardware	Mediatek	Mt8188	-	All	All	All
Hardware	Mediatek	Mt8195	-	All	All	All
Hardware	Mediatek	Mt8395	-	All	All	All
Hardware	Mediatek	Mt8781	-	All	All	All

References

Reference	Source	Link	Tags
September 2023	MISC	corp.mediatek.com	

CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.